PCT/JP2004/007112

日本国特許庁 19.05.2004
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

REC'D 08 JUL 2004
WIPO PCT

出願年月日
Date of Application: ２００３年　８月２９日

出願番号
Application Number: 特願２００３－３０７８７２

[ST. 10/C]: [ＪＰ２００３－３０７８７２]

出願人
Applicant(s): 北川　淑子

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年　６月２１日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００４－３０５５１０８

【書類名】　特許願
【整理番号】　I-MYU-17
【提出日】　平成15年 8月29日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/32
【発明者】
　【住所又は居所】　東京都渋谷区広尾２丁目３番１４号
　【氏名】　北川　高嗣
【特許出願人】
　【識別番号】　500285565
　【氏名又は名称】　北川　淑子
【代理人】
　【識別番号】　100083806
　【弁理士】
　【氏名又は名称】　三好　秀和
　【電話番号】　03-3504-3075
【選任した代理人】
　【識別番号】　100068342
　【弁理士】
　【氏名又は名称】　三好　保男
【選任した代理人】
　【識別番号】　100100712
　【弁理士】
　【氏名又は名称】　岩▲崎▼　幸邦
【選任した代理人】
　【識別番号】　100087365
　【弁理士】
　【氏名又は名称】　栗原　彰
【選任した代理人】
　【識別番号】　100100929
　【弁理士】
　【氏名又は名称】　川又　澄雄
【選任した代理人】
　【識別番号】　100095500
　【弁理士】
　【氏名又は名称】　伊藤　正和
【選任した代理人】
　【識別番号】　100101247
　【弁理士】
　【氏名又は名称】　高橋　俊一
【選任した代理人】
　【識別番号】　100098327
　【弁理士】
　【氏名又は名称】　高松　俊雄
【手数料の表示】
　【予納台帳番号】　001982
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1

【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0211891

【書類名】特許請求の範囲
【請求項１】
認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバにおいて、
前記認証情報を記憶した認証情報記憶装置と、
前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する認証画像生成手段と、
前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を、前記認証端末から取得する認証情報取得手段と、
前記認証パラメータ記憶装置を参照して、前記認証情報取得手段で取得した前記認証画像の情報が、前記認証画像生成手段で生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するか否かを判定し、その結果を前記通信端末に送信する認証情報照合手段
とを備えることを特徴とする情報処理サーバ。
【請求項２】
前記認証画像生成手段で生成する認証パラメータは、一意に特定できる乱数及び日時のいずれか一つ以上を含むことを特徴とする請求項１に記載の情報処理サーバ。
【請求項３】
前記認証画像生成手段において、前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、
前記認証情報照合手段において、前記認証情報取得手段によって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする
ことを特徴とする請求項１又は２に記載の情報処理サーバ。
【請求項４】
前記認証画像生成手段において、第１の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、
前記認証情報取得手段において、前記第１の通信ネットワークとは異なる第２の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する
ことを特徴とする請求項１乃至３のいずれか１項に記載の情報処理サーバ。
【請求項５】
前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした情報であることを特徴とする請求項１乃至４のいずれか１項に記載の情報処理サーバ。
【請求項６】
前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求項１乃至４のいずれか１項に記載の情報処理サーバ。
【請求項７】
前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求項１乃至６のいずれか１項に記載の情報処理サーバ。
【請求項８】
前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、
前記認証画像生成手段において、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、
前記認証情報照合手段において、前記結果を前記コンテンツ提供サーバに送信する
ことを特徴とする請求項１乃至７のいずれか１項に記載の情報処理サーバ。

【請求項９】
認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法において、
前記認証情報を認証情報記憶装置に記憶するステップと、
認証画像生成手段によって、前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する前記認証画像を生成するステップと、
認証情報取得手段によって、前記認証端末から、前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を取得するステップと、
認証情報照合手段によって、前記認証パラメータ記憶装置を参照して、前記認証画像の情報が、前記認証画像を生成するステップで生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するか否かを判定し、その結果を前記通信端末に送信する前記認証情報を照合するステップ
とを備えることを特徴とする情報処理方法。
【請求項１０】
前記認証画像を生成するステップで生成する認証パラメータは、一意に特定できる乱数及び日時のいずれか一つ以上を含むことを特徴とする請求項９に記載の情報処理方法。
【請求項１１】
前記認証画像を生成するステップにおいて、前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、
前記認証情報を照合するステップにおいて、前記認証情報を取得するステップによって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする
ことを特徴とする請求項９又は１０に記載の情報処理方法。
【請求項１２】
前記認証画像を生成するステップにおいて、第１の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、
前記認証情報を取得するステップにおいて、前記第１の通信ネットワークとは異なる第２の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する
ことを特徴とする請求項９乃至１１のいずれか１項に記載の情報処理方法。
【請求項１３】
前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした情報であることを特徴とする請求項９乃至１２のいずれか１項に記載の情報処理方法。
【請求項１４】
前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求項９乃至１２のいずれか１項に記載の情報処理方法。
【請求項１５】
前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求項９乃至１４のいずれか１項に記載の情報処理方法。
【請求項１６】
前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、
前記認証画像を生成するステップにおいて、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、
前記認証情報を照合するステップにおいて、前記結果を前記コンテンツ提供サーバに送

信する
ことを特徴とする請求項９乃至１５のいずれか１項に記載の情報処理方法。

【書類名】明細書
【発明の名称】情報処理サーバ及び情報処理方法
【技術分野】
【０００１】
本発明は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理サーバ及び情報処理方法に関する。
【背景技術】
【０００２】
現在、インターネットと携帯端末の普及によりいつでもどこでも情報通信を行えるようになってきている。そのため通信される情報が他人に漏れないように様々な暗号化が考えられており、暗号化されたＨＴＴＰＳ（Hypertext Transfer Protocol Security）などのプロトコルを利用して情報をサーバに送信することも頻繁に行われている。
【０００３】
携帯端末の場合、規格が通信事業者によって決まるため、例えば、携帯端末を識別する機器識別子を取得することにより、サーバは携帯端末の認証を高い精度で行うことができる。
【０００４】
しかし、インターネット等の通信ネットワークにおいて、コンピュータ等の認証を行うことは困難とされている。即ち、コンピュータでインターネット等に接続するために利用するブラウザやＨＴＴＰ（Hypertext Transfer Protocol）などのプロトコルによれば、携帯端末の様に、コンピュータを識別する識別子を取得しサーバに送信することが不可能である。実際は、ブラウザのクッキーにサーバが作成した暗号化された暗号文を記憶し、認証時にその暗号文をサーバに送信したり、サーバへの接続時にユーザにパスワードを入力させるなどの方法が一般的である。
【０００５】
Ｗｅｂ上の提携サイトとネットワークを介して接続され、提携サイトへのアクセスが許容されたユーザの認証情報を格納するユーザ情報データベースと、提携サイトへ入力された認証情報を取得し、ユーザ情報データベースに基づいて認証処理を行い、認証結果を提携サイトへ送信する制御手段とを備えた認証システムなどがある（例えば特許文献１）。
【特許文献１】特開２００３－６１６４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかし上述した特許文献１においては、認証システムにおいてのみ認証されれば、複数の提携サイトについての認証は必要ないが、認証システムにおける認証において盗聴された場合、ユーザの損失は計り知れないものがある。
【０００７】
一方、携帯電話機などの携帯端末の普及に伴い、携帯電話を利用して様々なサービスを享受するユーザが多く、サービスの提供時には氏名、住所などの個人情報を登録する場合がある。この場合、入力するユーザインタフェースに乏しい携帯端末においてこれらの個人情報を登録するのは非常に困難であり、コンピュータでの登録を望むユーザも多い。しかしコンピュータでの登録においては、上述したようなユーザ認証時の問題があり、これを打破するシステムの開発が望まれている。
【０００８】
従って本発明の目的は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理サーバ及び情報処理方法を提供することである。
【課題を解決するための手段】
【０００９】
上記課題を解決するために、本発明は、認証端末が備える認証情報を利用して、認証情

報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバにおいて、認証情報を記憶した認証情報記憶装置と、通信端末の認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証パラメータ記憶装置に記憶する認証画像生成手段と、通信端末から取得した認証画像の情報と、認証端末が備える認証情報を、認証端末から取得する認証情報取得手段と、認証パラメータ記憶装置を参照して、認証情報取得手段で取得した認証画像の情報が、認証画像生成手段で生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報照合手段とを備える。

【００１０】

このような本発明によれば、認証情報を持たない端末でも、認証情報を用いることにより認証を受けることができる。

【００１１】

又、認証画像生成手段で生成する認証パラメータは、一意に特定できる乱数及び日時のいずれか一つ以上を含むことが好ましい。

【００１２】

この場合、情報処理サーバで生成した認証パラメータを推測しにくくなるので、より高いセキュリティレベルを保証することができる。

【００１３】

又、認証画像生成手段において、認証パラメータ記憶装置に、認証パラメータの有効日時を更に記憶し、認証情報照合手段において、認証情報取得手段によって取得した日時が、認証パラメータ記憶装置に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にすることが好ましい。

【００１４】

これによると、認証の有効日時を設けることにより、通信端末と認証端末の間で不正が行われたとしても、その認証を排除することができる。

【００１５】

又、認証画像生成手段において、第１の通信ネットワークを利用して通信端末に認証画像を送信し、認証情報取得手段において、第１の通信ネットワークとは異なる第２の通信ネットワークを利用して認証端末から認証画像の情報と認証情報を取得することが好ましい。

【００１６】

これによると、別々のネットワークで認証画像と認証情報の送受信を行うので、ネットワークの盗聴が行われても、両方の情報を取得することは非常に困難になる。

【００１７】

又、認証画像の情報は、通信端末から取得した認証画像を、認証端末においてデコードした情報であることが好ましい。又、認証画像の情報は、通信端末から取得し、認証端末から受信した認証画像を、デコードした情報であることが好ましい。

【００１８】

このような、本発明において送受信される認証情報は、必要な情報が含まれていれば良く、その形態は問わない。

【００１９】

又、通信端末から認証画像の情報を取得する場合、認証端末によって、通信端末に提示された認証画像を撮影しデコードすることが好ましい。

【００２０】

これによると、認証画像を撮影し、認証端末３でデコードすることにより、ユーザは容易に認証画像を認証端末３に取り込むことができる。又、このデコード時には、認証端末に記憶されたキーを元に復号しても良い。

【００２１】

又、情報処理システムは、通信端末にコンテンツを提供するコンテンツ提供サーバを更

に備えており、認証画像生成手段において、コンテンツ提供サーバから、通信端末の認証依頼を受信し、認証情報照合手段において、結果をコンテンツ提供サーバに送信することが好ましい。

【００２２】

これによると、情報処理サーバ以外のサーバにおいても、本発明の情報処理サーバの認証機能を用いることにより、高いセキュリティレベルで通信端末を認証することができる。

【００２３】

本発明は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法において、認証情報を認証情報記憶装置に記憶するステップと、認証画像生成手段によって、通信端末の認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証パラメータ記憶装置に記憶する認証画像を生成するステップと、認証情報取得手段によって、認証端末から、通信端末から取得した認証画像の情報と、認証端末が備える認証情報を取得するステップと、認証情報照合手段によって、認証パラメータ記憶装置を参照して、認証画像の情報が、認証画像を生成するステップで生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報を照合するステップとを備える。

【００２４】

又、認証画像を生成するステップで生成する認証パラメータは、一意に特定できる乱数及び日時のいずれか一つ以上を含むことが好ましい。

【００２５】

又、認証画像を生成するステップにおいて、認証パラメータ記憶装置に、認証パラメータの有効日時を更に記憶し、認証情報を照合するステップにおいて、認証情報を取得するステップによって取得した日時が、認証パラメータ記憶装置に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にすることが好ましい。

【００２６】

又、認証画像を生成するステップにおいて、第１の通信ネットワークを利用して通信端末に認証画像を送信し、認証情報を取得するステップにおいて、第１の通信ネットワークとは異なる第２の通信ネットワークを利用して認証端末から認証画像の情報と認証情報を取得することが好ましい。

【００２７】

又、認証画像の情報は、通信端末から取得した認証画像を、認証端末においてデコードした情報であることが好ましい。

【００２８】

又、認証画像の情報は、通信端末から取得し、認証端末から受信した認証画像を、デコードした情報であることが好ましい。

【００２９】

又、通信端末から認証画像の情報を取得する場合、認証端末によって、通信端末に提示された認証画像を撮影しデコードすることが好ましい。

【００３０】

又、情報処理システムは、通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、認証画像を生成するステップにおいて、コンテンツ提供サーバから、通信端末の認証依頼を受信し、認証情報を照合するステップにおいて、結果をコンテンツ提供サーバに送信することが好ましい。

【発明の効果】

【００３１】

本発明によれば、認証端末が備える認証情報を利用して、認証情報を備えない通信端末

を認証する情報処理サーバ及び情報処理方法を提供することができる。
【発明を実施するための最良の形態】
【００３２】
これによると、
次に、図面を参照して、本発明の実施の形態を説明する。以下の図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。
【００３３】
（第１の実施の形態）
図１を参照して、本発明の第１の実施の形態に係る情報処理サーバ１と、情報処理サーバ１を利用した情報処理システムについて説明する。情報処理サーバ１は、中央処理制御装置、メモリなどを備える一般的なコンピュータに所定の処理を実行するソフトウェアプログラムをインストールすることによって実現される。
【００３４】
本発明の情報処理サーバ１は、認証端末３が備える認証情報を利用して、認証情報を備えない通信端末２を認証する。ここで、通信端末２は、一般的なコンピュータで、認証端末３は、認証情報を備えた携帯電話機などの通信端末である。認証情報は、指紋認証情報なのでも良いが、本実施の形態においては、情報処理サーバ１が発行した暗号化され改竄不可能な認証識別子であるとする。
【００３５】
本発明の実施の形態に係る情報処理システムにおいて、情報処理サーバ１は、第１の通信ネットワーク４ａを介して通信端末２と互いに接続可能で、更に、第２の通信ネットワーク４ｂを介して認証端末３と互いに接続可能である。第１の通信ネットワーク４ａと第２の通信ネットワーク４ｂは、少なくとも一部が互いに交差しない通信ネットワークである。
【００３６】
本発明の実施の形態に係る情報処理サーバ１は、認証パラメータ記憶装置１０１、認証情報記憶装置１０２、認証識別子記憶装置１０３、認証画像生成手段１１１、認証情報取得手段１１２、認証情報照合手段１１３、入出力制御手段１２１を備えている。
【００３７】
認証識別子記憶装置１０３は、情報処理サーバ１が発行した認証端末３を認証するための認証識別子（認証情報）を記憶した記憶装置である。
【００３８】
認証画像生成手段１１１は、通信端末２の認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末２に送信し、認証パラメータを認証パラメータ記憶装置１０１に記憶する手段である。
【００３９】
ここで、認証画像生成手段１１１で生成し、認証パラメータ記憶装置１０１に記憶される認証パラメータは、一意に特定できるワンタイムパスワードの様な乱数及び日時のいずれか一つ以上を含む情報である。この認証パラメータの「日時」は、認証パラメータ生成時の日時でも良いし、通信端末２の認証依頼を受信した日時でも良い。又、認証パラメータ記憶装置１０１には、認証パラメータを有効にする期限である有効日時も記憶していても良い。認証画像生成手段１１１は、第１の通信ネットワーク４ａを介して通信端末２に認証画像を送信する。ここでは認証画像を送信すると記載したが、認証端末３において情報を解読できれば、テキストでも構わない。テキストの場合、簡単に盗聴できないような桁数の多いものが好ましい。
【００４０】
認証情報取得手段１１２は、通信端末２から取得した認証画像の情報と、認証端末３が備える認証情報を、認証端末３から取得し、認証情報記憶装置１０２に記憶する手段である。認証情報取得手段１１２は、第２の通信ネットワーク４ｂを介して認証端末３から認証情報を受信する。ここで、認証画像の情報は、通信端末２から取得した認証画像を、認

証端末３においてデコードした情報であっても良いし、通信端末２から取得し、認証端末３から受信した認証画像を、情報処理サーバ１においてデコードした情報であっても良い。更に、通信端末２から認証画像の情報を取得する場合、認証端末３によって、通信端末２に提示された認証画像を撮影しデコードしても良い。又、通信端末２と認証端末３の間で赤外線通信などの近距離無線通信を利用したり、リムーバブルディスクを利用して、認証端末３は認証画像を取得しても良い。

【００４１】

認証情報照合手段１１３は、認証パラメータ記憶装置１０１と認証情報記憶装置１０２と認証識別子記憶装置１０３を参照して、認証情報取得手段１１２で取得した認証画像の情報が、認証画像生成手段１１１で生成された画像の情報であり、更に、認証端末３が備える認証情報が、認証識別子記憶装置１０３に記憶した認証情報と一致するか否かを判定し、その結果を通信端末２に送信する手段である。更に、認証パラメータ記憶装置１０１において、認証パラメータの有効日時が記憶されている場合、認証情報取得手段１１２で取得した日時が、認証パラメータ記憶装置１０１に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にしても良い。

【００４２】

入出力制御手段１２１は、情報処理サーバ１の入力や出力を制御し、それぞれのネットワークや手段にその情報を伝達する手段である。

【００４３】

本発明の実施の形態に係る通信端末２は、認証画像データ記憶装置２０１、認証画像取得手段２１１、認証画像提示手段２１２、認証結果取得手段２１３を備えている。

認証画像取得手段２１１は、情報処理サーバ１の認証画像生成手段１１１によって生成された認証画像を取得し、認証画像データ記憶装置２０１に記憶する手段である。

認証画像提示手段２１２は、認証画像データ記憶装置２０１に記憶された認証画像データを認証端末３に提示する手段である。

更に、認証結果取得手段２１３は、情報処理サーバ１の認証情報照合手段１１３によって送信された認証の結果を取得する手段である。

【００４４】

本発明の実施の形態に係る認証端末３は、認証画像データ記憶装置３０１、認証識別子記憶装置３０２、認証画像撮影手段３１１、認証情報送信手段３１２を備えている。

認証画像撮影手段３１１は、通信端末２の認証画像提示手段２１２によって提示された画像を撮影し、認証画像データ記憶装置３０１に記憶する手段である。画像を撮影する必要はなく、通信端末２に送信された認証画像を認証端末３に取得できればどのような手段を用いても構わない。

認証情報送信手段３１２は、認証識別子記憶装置３０２に記憶された、情報処理サーバ１から取得した認証識別子と、認証画像データ記憶装置３０１に記憶された画像の情報を第２の通信ネットワーク４ｂを介して情報処理サーバ１に送信する手段である。

【００４５】

次に、図２を参照して本発明の第１の実施の形態に係る情報処理方法を説明する。

【００４６】

まず、ステップＳ１０１において情報処理サーバ１は、認証画像生成手段１１１によって、通信端末２から認証依頼を受信すると、ステップＳ１０２において、ワンタイムパスワードや日時などの情報を含む認証画像を生成し、認証パラメータ記憶装置１０１に記憶する。更にステップＳ１０３において、情報処理サーバ１は、生成した認証画像を通信端末２に送信する。

通信端末２は、ステップＳ１０３において認証画像を受信すると、受信した画像をステップＳ１０４において提示する。

ステップＳ１０４において通信端末２で認証画像が提示されると、ステップＳ１０５において認証端末３は提示された認証画像を撮影し、認証画像データ記憶装置３０１に記憶

する。更にステップＳ１０６において認証端末３は、認証画像データ記憶装置３０１に記憶された認証画像の情報と、認証識別子記憶装置３０２に記憶された認証端末３の認証識別子を併せて認証情報を作成し、ステップＳ１０７において、認証情報を情報処理サーバ１０７に送信する。

【００４７】

ステップＳ１０７において、情報処理サーバ１は認証端末３から認証情報を受信すると、認証情報取得手段１１２によって、受信した認証情報を認証情報記憶装置１０２に記憶し、ステップＳ１０８において認証情報照合手段１１３によって認証パラメータ記憶装置１０１、認証情報記憶装置１０２、認証識別子記憶装置１０３を参照して認証情報の照合を行う。

認証情報の認証結果が出ると、情報処理サーバ１は、通信端末２に認証結果を送信し、通信端末２は認証結果取得手段２１３によって認証結果を受信する。

【００４８】

本発明の第１の実施の形態に係る情報処理サーバ１によると、認証端末３の認証情報を利用することにより、認証情報を備えていない通信端末２を認証することができる。従って、ユーザは一つの認証端末３を備えていれば、複数の端末について同様に認証を受けることができる。

【００４９】

更に、本発明の第１の実施の形態によれば、本来は携帯電話機で入力しなければならない情報を、ユーザインタフェースの充実しているコンピュータで入力し、更に、セキュリティレベルの高い状態で、その入力した情報をサーバに送信することができる。

【００５０】

（第２の実施の形態）

図３に示した本発明の第２の実施の形態に係る情報処理システムは、図１に示した本発明の第１の実施の形態に係る情報処理システムに比べて、コンテンツ提供サーバ５を備えている点が異なる。更に、通信端末２において、認証結果取得手段２１３を備えておらず、コンテンツ取得手段２１４を備えている点が異なる。

【００５１】

本発明の第２の実施の形態に係る情報処理サーバ１は、認証画像生成手段１１１において、コンテンツ提供サーバ５から、通信端末２の認証依頼を受信し、認証情報照合手段１１３において、結果をコンテンツ提供サーバ５に送信する。

【００５２】

本発明の第２の実施の形態に係るコンテンツ提供サーバ５は、情報処理サーバ１及び認証端末３の情報を利用して通信端末２を認証し、認証された通信端末２にコンテンツを配信するものであって、コンテンツ記憶装置５０１、認証依頼手段５１１、認証結果取得手段５１２、コンテンツ配信手段５１３を備えている。

コンテンツ記憶装置５０１は、コンテンツ提供サーバ５が提供するコンテンツが記憶された記憶装置である。

認証依頼手段５１１は、例えば通信端末２からコンテンツの取得依頼があると、情報処理サーバ１に対して、通信端末２の認証を依頼する手段である。

認証結果取得手段５１２は、認証依頼手段５１１で依頼した通信端末２の認証結果を、情報処理サーバ１から取得する手段である。

コンテンツ配信手段５１３は、通信端末２が認証されると、コンテンツ記憶装置５０１に記憶されたコンテンツを通信端末２に送信する手段である。

【００５３】

図３においては、本発明の第２の実施の形態に係るコンテンツ提供サーバ５は、第１の通信ネットワーク４ａに接続されているが、情報処理サーバ１と相互に通信可能ならば、どの通信ネットワークに接続されても良い。

【００５４】

図４を参照して、本発明の第２の実施の形態に係る情報処理方法を説明する。

まず、ステップＳ２０２において、通信端末２からコンテンツ提供サーバ５にコンテンツの要求がされると、コンテンツ提供サーバ５は、ステップＳ２０２において認証依頼手段５１１によって、情報処理サーバ１に通信端末２の認証を依頼する。

その後、ステップＳ２０３乃至ステップ２０９の処理は、図２のステップＳ１０２乃至ステップＳ１０８の処理と同様なので説明を割愛する。

【００５５】

ステップＳ２０９において、情報処理サーバ１において認証結果が出ると、情報処理サーバ１はステップＳ２１０において、通信端末２の認証結果をコンテンツ提供サーバ５に送信する。

コンテンツ提供サーバ５は、認証が許可されると、ステップＳ２１１においてコンテンツ記憶装置５０１から通信端末２にコンテンツを提供する。

この方法は、通信端末２において一般的なブラウザを利用してコンテンツ提供サーバ５からコンテンツを取得する場合に有効である。

【００５６】

次に、図５を参照して、本発明の第２の実施の形態の変形例に係る情報処理方法について説明する。

まず、ステップＳ２５１において、通信端末２がコンテンツ提供サーバ５にコンテンツを要求すると、ステップＳ２５２において、コンテンツ提供サーバ５は、通信端末２に認証情報を要求する。

これを受けて通信端末２は、ステップＳ２５３において情報処理サーバ１に認証依頼を行う。

その後、ステップＳ２５４乃至ステップ２６０の処理は、図２のステップＳ１０２乃至ステップＳ１０８の処理と同様なので説明を割愛する。

ステップＳ２６０において、情報処理サーバ１において認証結果が出ると、情報処理サーバ１はステップＳ２６１において、通信端末２の認証結果を通信端末２に送信し、これを受けて通信端末２は、ステップＳ２６２において認証結果をコンテンツ提供サーバ５に送信する。

コンテンツ提供サーバ５は、認証結果を受信すると、認証が許可されている場合、ステップＳ２６３においてコンテンツ記憶装置５０１から通信端末２にコンテンツを提供する。

この方法は、通信端末２ににおいて、コンテンツ提供サーバ５や情報処理サーバ１が提供する認証依頼プログラムを含むアプリケーションによって、コンテンツ提供サーバ５にコンテンツを提供する場合に有効である。

【００５７】

本発明の第２の実施の形態によれば、情報処理サーバ１は、複数のサーバの認証機能を受け付けることができ、様々なサーバに高いセキュリティレベルの認証を行わせることができる。

【００５８】

（第３の実施の形態）

本発明の第１及び第２の実施の形態においては、通信端末２の認証について主に説明したが、本発明の第３の実施の形態においては、通信端末２及び認証端末３を操作するユーザの認証について説明する。

【００５９】

図６に示す本発明の第３の実施の形態に係る情報処理サーバ１は、図１に示す本発明の第１の実施の形態に係る情報処理サーバ１と比べて、リマインダー質疑応答記憶装置１０４、リマインダー質疑応答登録手段１１４、パスワード再発行手段１１５を備えている点が異なる。更に、第３の実施の形態に係る認証端末３は、第１の実施の形態に係る認証端末３に比べて、リマインダー質疑応答登録手段３１３、再発行パスワード取得手段３１４を備えている点が異なる。

【００６０】

リマインダー質疑応答登録手段１１４は、認証端末３のリマインダー質疑応答登録手段３１３によって複数ある質疑応答のうち、ユーザにユーザが答えられる複数の質疑応答を選択させ、ユーザの認証識別子に関連づけて、そのユーザが選択した質疑応答とその答えをリマインダー質疑応答記憶装置１０４に記憶する手段である。

【００６１】

パスワード再発行手段１１５は、ユーザがパスワードを忘れてしまった場合、認証端末３の再発行パスワード取得手段３１４によってパスワードの再発行が要求されると、リマインダー質疑応答記憶装置１０４を参照してユーザが選択した質問をユーザに答えさせ、リマインダー質疑応答記憶装置１０４に記憶された応答と一致するかを判定し、全ての質疑に答えられた場合、ユーザにパスワードを発行する手段である。

【００６２】

図７に示すように、本発明の第３の実施の形態の情報処理サーバ１が提示する複数の質疑応答は、質疑の候補、応答のセレクトリストの項目を備えている。更に、質疑のジャンルとセレクトリストのセレクト数の項目を備えていても良い。ユーザはこれらの質疑の候補の中から、ユーザ自身が確実に答えられる質問を所定の数（例えば４つなど）以上を、ユーザに選択させる。このようにユーザが登録時に４問以上選択することになる場合、１１問から４問以上を選択する組み合わせの数は、１８１７通りとなる。

【００６３】

例えば、「お母さんは何日生まれ？」という質問がユーザに選択されたとすると、セレクトリストとしては１～３１日が挙げられ、ユーザはその中から正解を選択する。これらを所定の数だけ繰り返し、認証端末３は、情報処理サーバ１に送信する。例えば、選択数１５の質疑をユーザが４つ選択したとすると、その回答の組合せは、１５の４乗となり、５０６２５通りにも及ぶ。このような方法を取ることにより、ユーザの選択した質疑とその応答を解読するのは不可能になり、より高いセキュリティレベルを保つことができる。

【００６４】

例えば、図８に示すように、英数字だけのパスワードによると、英数字（Ａ～Ｚまでの英字２６文字と０から９までの数字１０個）を組合せると、３６文字の４乗で１，６７９，６１６通りあることを示す。

【００６５】

一方、本発明の第３の実施の形態で説明した方法によると、図７に示す様に１１の質問から４つを選択し、その４つについて５０，６２５通りのセレクトリストの組合せがあるとすると、ユーザがとりうる組合せは、少なく見積もっても９１，９８５，６２５通り以上となる。これは、図８を参照すると分かるように、英数字のみをパスワードにした場合、５～６桁の、数字のみをパスワードにした場合、７～８桁の強度があることが分かる。

【００６６】

図９を参照して、本発明の第３の実施の形態に係る情報処理方法について説明する。

まず、リマインダー質疑応答を登録する場合、ステップＳ３０１において情報処理サーバ１は認証端末３に質問と、回答の選択肢の組合せを送信し、ユーザに確実に回答できる質問とその答えを決定させる。次に、ステップＳ３０２において、情報処理サーバ１は認証端末３から、所定の数以上の質問と回答の組合せを受信し、リマインダー質疑応答記憶装置１０４に記憶する。

更にパスワードを再発行する場合、ステップＳ３５１において、情報処理サーバ１は認証端末３からパスワードの再発行依頼を受信すると、ステップＳ３５２において、情報処理サーバ１は認証端末３に、ステップＳ３０１で送信した質問と回答の選択肢の組合せと同じものを送信し、ユーザにステップＳ３０２で回答した質問に回答させる。

更に、ステップＳ３５３において、認証端末３から登録時に回答した質問と回答の組合せを受信すると、ステップＳ３５４においてリマインダー質疑応答記憶装置１０４を参照して回答を照合し、照合の結果、選択した質問と、その質問の回答の全てが一致していた場合、ステップＳ３５３においてパスワードを再発行する。

【００６７】

本発明の第３の実施の形態に係る情報処理システムによれば、非常に高いセキュリティレベルでユーザを認証することができる。

【００６８】

上記のように、本発明の第１乃至第３の実施の形態によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施の形態、実施例及び運用技術が明らかとなる。

【００６９】

本発明はここでは記載していない様々な実施の形態等を含むことは勿論である。従って、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。

【図面の簡単な説明】

【００７０】

【図１】本発明の第１の実施の形態に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

【図２】本発明の第１の実施の形態に係る情報処理方法を示すシーケンス図である。

【図３】本発明の第２の実施の形態に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

【図４】本発明の第２の実施の形態に係る情報処理方法を示すシーケンス図である。

【図５】本発明の第２の実施の形態の変形例に係る情報処理方法を示すシーケンス図である。

【図６】本発明の第３の実施の形態に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

【図７】本発明の第３の実施の形態に係る情報処理サーバがユーザに提示する質問リストとそのセレクトリストの一例である。

【図８】従来のパスワードによる認証の場合の組合せを示した図である。

【図９】本発明の第３の実施の形態に係る情報処理方法を示すシーケンス図である。

【符号の説明】

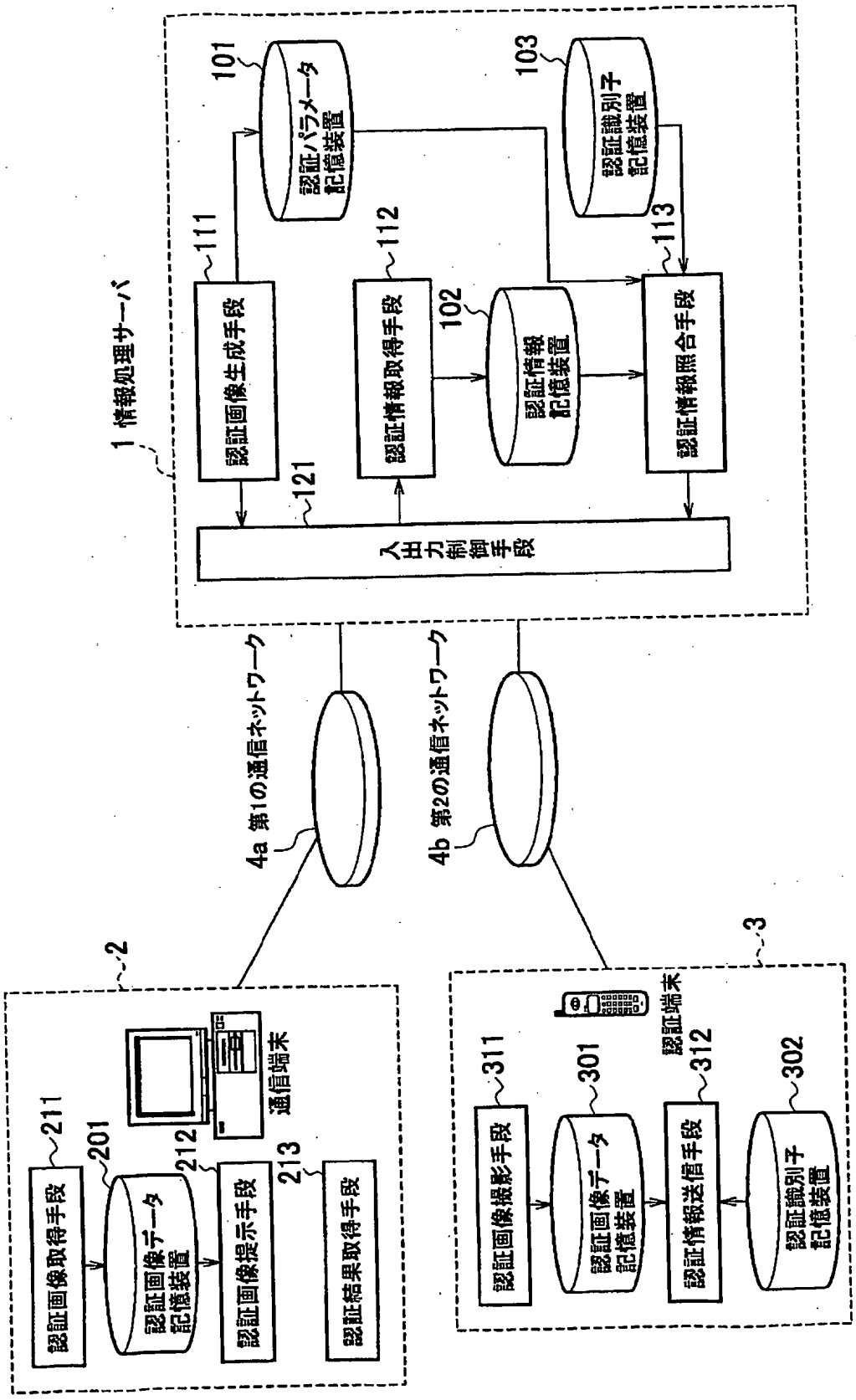
【００７１】

１…情報処理サーバ
２…通信端末
３…認証端末
４ａ、４ｂ…通信ネットワーク
１０１…認証パラメータ記憶装置
１０２…認証情報記憶装置
１０３…認証識別子記憶装置
１０４…リマインダー質疑応答記憶装置
１０７…情報処理サーバ
１１１…認証画像生成手段
１１２…認証情報取得手段
１１３…認証情報照合手段
１１４…リマインダー質疑応答登録手段
１１５…パスワード再発行手段
１２１…入出力制御手段
２０１…認証画像データ記憶装置
２１１…認証画像取得手段
２１２…認証画像提示手段
２１３…認証結果取得手段
２１４…コンテンツ取得手段
３０１…認証画像データ記憶装置
３０２…認証識別子記憶装置

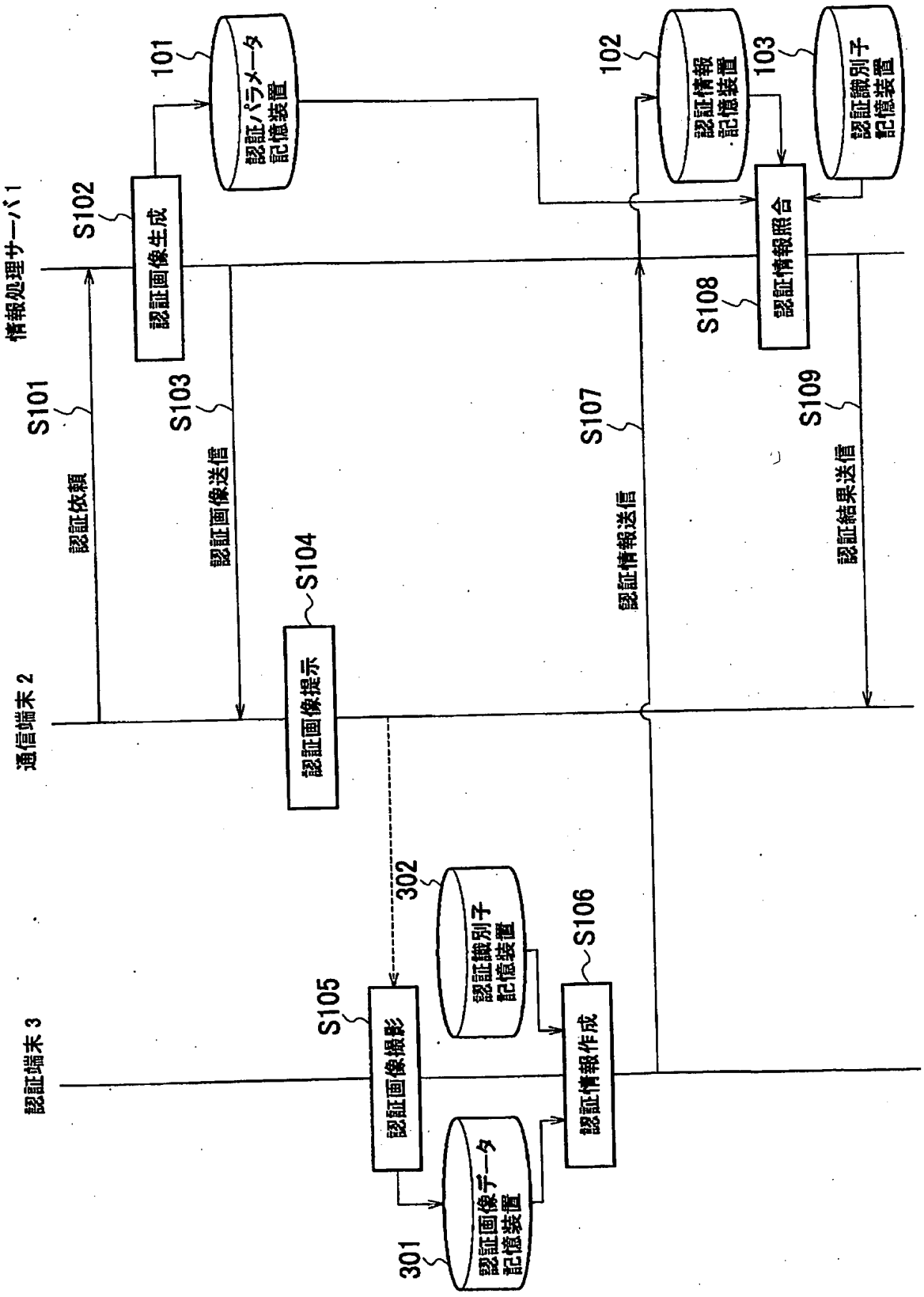
３１１…認証画像撮影手段
３１２…認証情報送信手段
３１３…リマインダー質疑応答登録手段
３１４…再発行パスワード取得手段
５０１…コンテンツ記憶装置
５１１…認証依頼手段
５１２…認証結果取得手段
５１３…コンテンツ配信手段

【書類名】図面

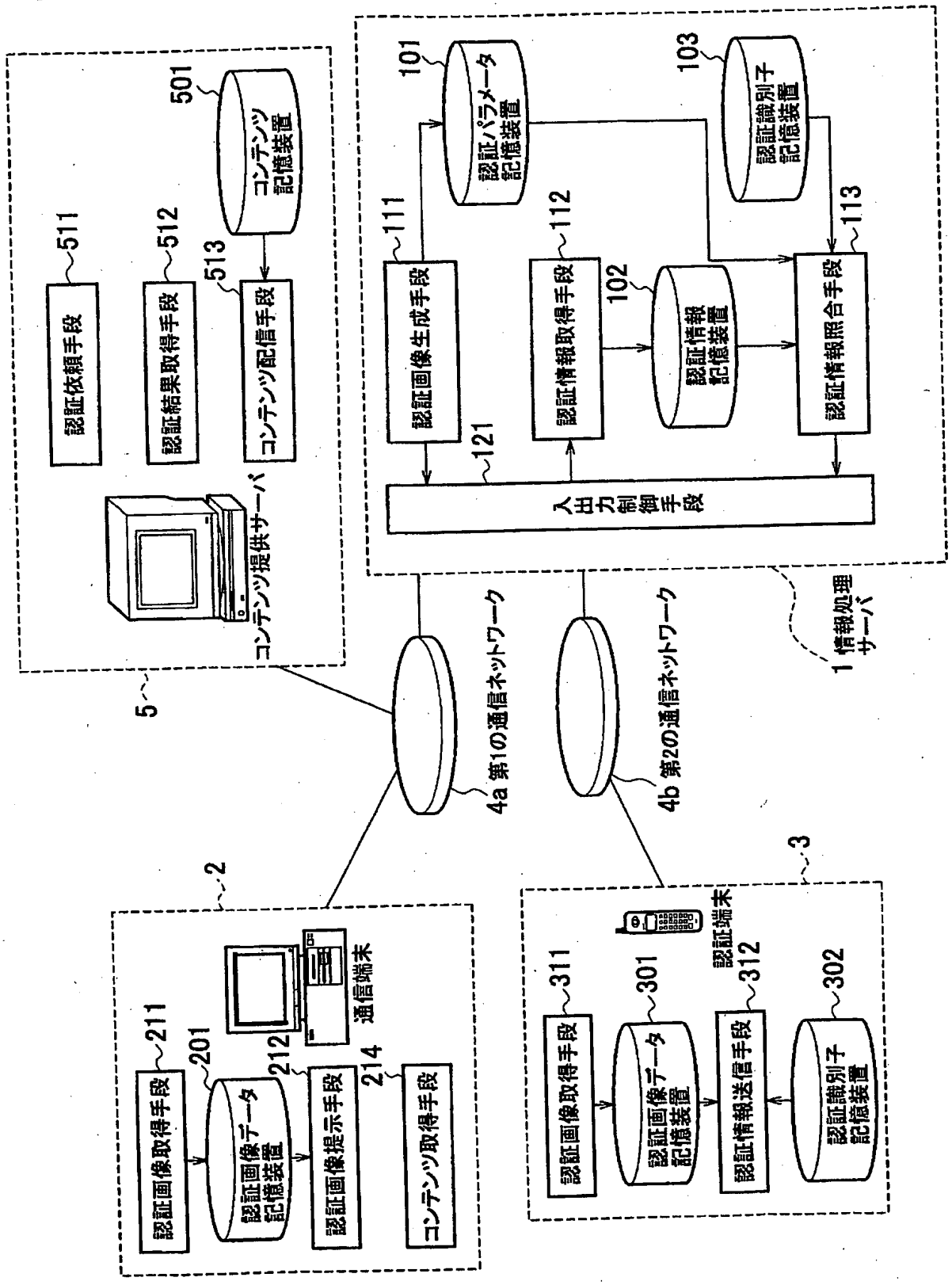
【図１】


1 情報処理サーバ
101
認証パラメータ記憶装置
103
認証識別子記憶装置
111
認証画像生成手段
112
認証情報取得手段
102
認証情報記憶装置
113
認証情報照合手段
121
入出力制御手段
4a 第1の通信ネットワーク
4b 第2の通信ネットワーク
2
211
認証画像取得手段
201
認証画像データ記憶装置
212
認証画像提示手段
213
認証結果取得手段
通信端末
3
311
認証画像撮影手段
301
認証画像データ記憶装置
312
認証情報送信手段
302
認証識別子記憶装置
認証端末

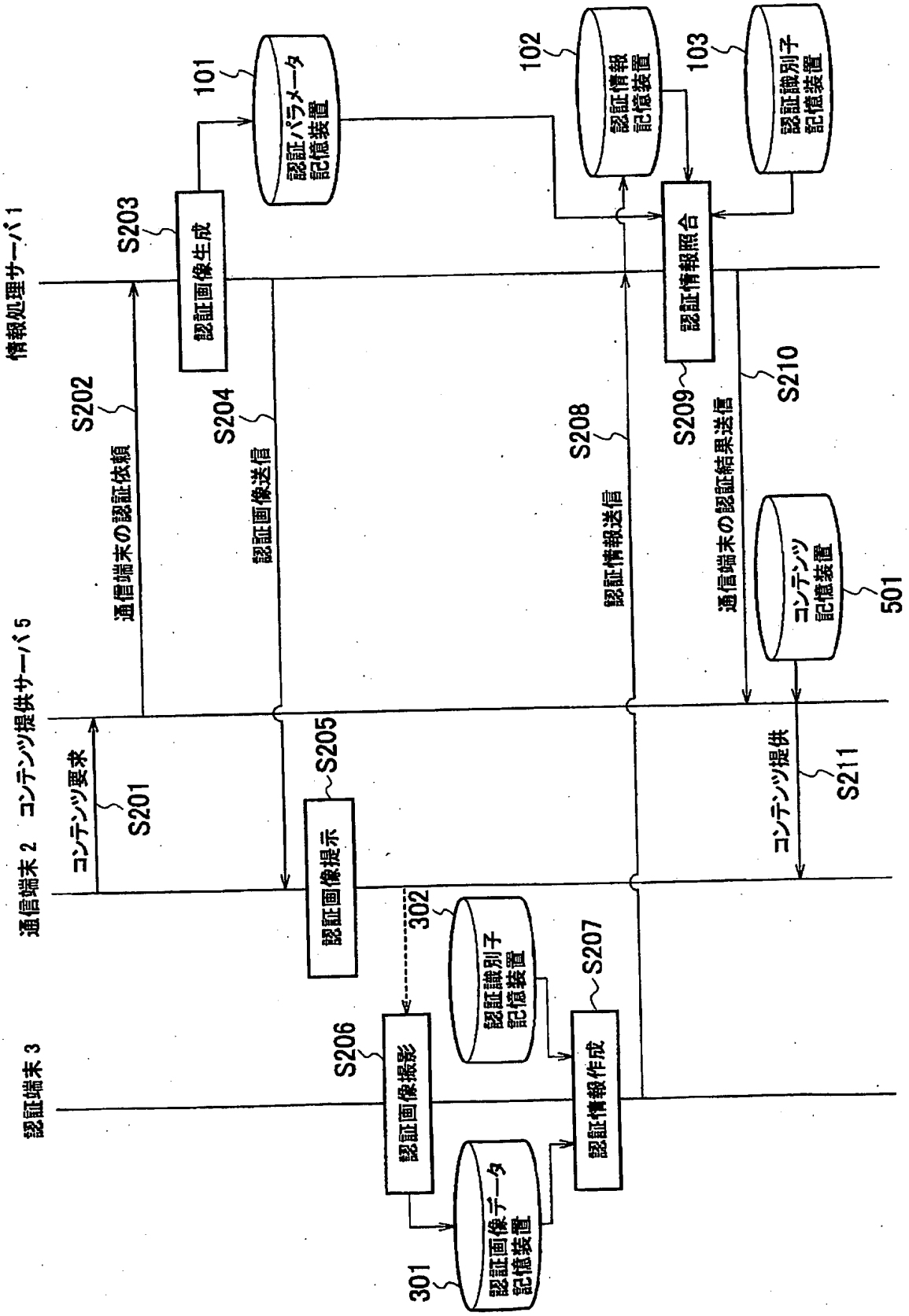
【図２】


情報処理サーバ１
通信端末２
認証端末３
S101
認証依頼
S102
認証画像生成
S103
認証画像送信
S104
認証画像提示
S105
認証画像撮影
S106
認証情報作成
S107
認証情報送信
S108
認証情報照合
S109
認証結果送信
101
認証パラメータ記憶装置
102
認証情報記憶装置
103
認証識別子記憶装置
301
認証画像データ記憶装置
302
認証識別子記憶装置

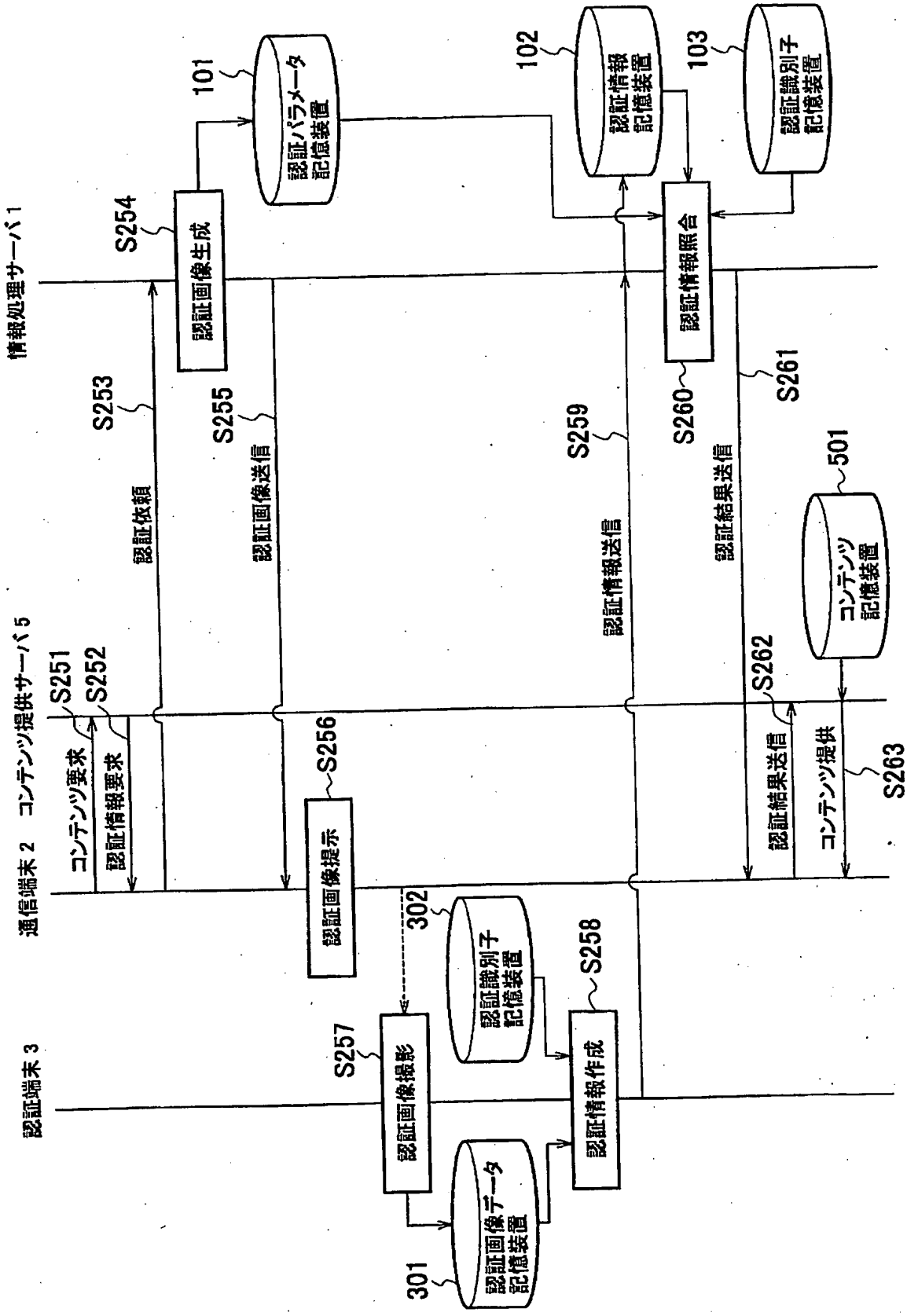
【図３】


1 情報処理サーバ
101 認証パラメータ記憶装置
103 認証識別子記憶装置
111 認証画像生成手段
112 認証情報取得手段
102 認証情報記憶装置
113 認証情報照合手段
121 入出力制御手段
501 コンテンツ記憶装置
511 認証依頼手段
512 認証結果取得手段
513 コンテンツ配信手段
コンテンツ提供サーバ
5
4a 第1の通信ネットワーク
4b 第2の通信ネットワーク
2
211 認証画像取得手段
201 認証画像データ記憶装置
212 認証画像提示手段
214 コンテンツ取得手段
通信端末
3
311 認証画像取得手段
301 認証画像データ記憶装置
312 認証情報送信手段
302 認証識別子記憶装置
認証端末

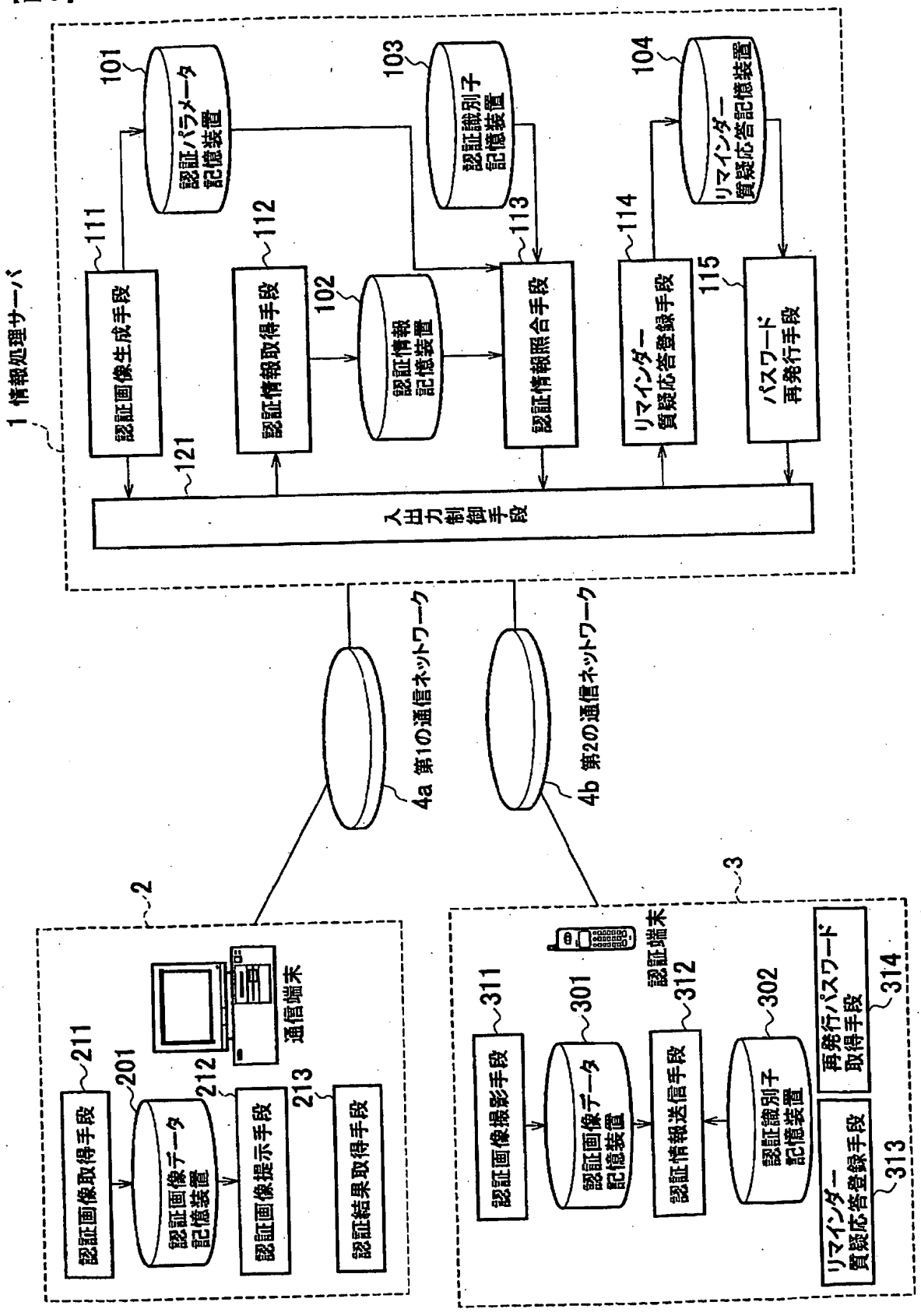
【図４】


情報処理サーバ１
通信端末２　コンテンツ提供サーバ５
認証端末３
認証画像生成
認証パラメータ記憶装置
認証情報照合
認証情報記憶装置
認証識別子記憶装置
コンテンツ記憶装置
認証画像提示
認証画像撮影
認証画像データ記憶装置
認証情報作成
コンテンツ要求
通信端末の認証依頼
認証画像送信
認証情報送信
通信端末の認証結果送信
コンテンツ提供
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210
S211
101
102
103
301
302
501

【図５】


情報処理サーバ１
通信端末２　コンテンツ提供サーバ５
認証端末３
101
認証パラメータ記憶装置
102
認証情報記憶装置
103
認証識別子記憶装置
S254
認証画像生成
S253
認証依頼
S255
認証画像送信
S259
認証情報送信
S260
認証情報照合
S261
認証結果送信
501
コンテンツ記憶装置
S251
コンテンツ要求
S252
認証情報要求
S256
認証画像提示
S262
認証結果送信
S263
コンテンツ提供
302
認証識別子記憶装置
S257
認証画像撮影
S258
認証情報作成
301
認証画像データ記憶装置

【図6】


1 情報処理サーバ
101
認証パラメータ記憶装置
103
認証識別子記憶装置
104
リマインダー質疑応答記憶装置
111
認証画像生成手段
112
認証情報取得手段
102
認証情報記憶装置
113
認証情報照合手段
114
リマインダー質疑応答登録手段
115
パスワード再発行手段
121
入出力制御手段
4a 第1の通信ネットワーク
4b 第2の通信ネットワーク
2
211
認証画像取得手段
201
認証画像データ記憶装置
212
認証画像提示手段
213
認証結果取得手段
通信端末
3
311
認証画像撮影手段
301
認証画像データ記憶装置
認証端末
312
認証情報送信手段
302
認証識別子記憶装置
再発行パスワード取得手段
314
リマインダー質疑応答登録手段
313

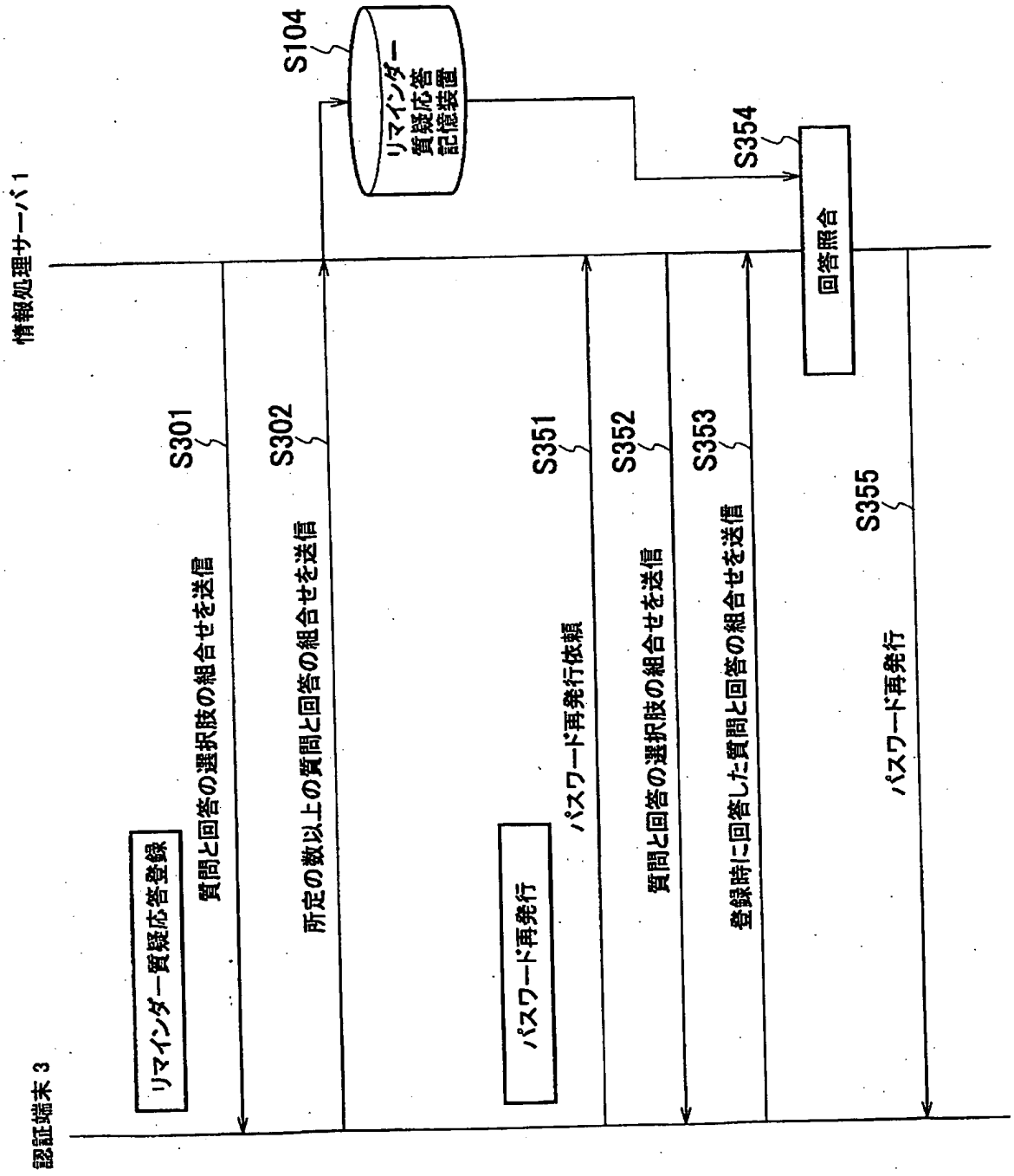
【図７】

	候補	ジャンル	セレクトリスト	セレクト数
1	お母さんは何日生まれ？	家族	1～31日	31
2	お父さんは何日生まれ？	家族	1～31日	31
3	母親(父親)の旧姓の頭文字は？	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
4	あなたの生まれた市区町村の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
5	初恋の人の苗字の頭文字は？	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
6	最初に飼ったペットの名前の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
7	初めて観た映画のタイトルの頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
8	尊敬する人の苗字の頭文字は？	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
9	母方の祖父の下の名前の頭文字は？	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
10	いとこは何人いる？	家族	0～14、15以上	16
11	初めての担任の先生の苗字の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15

【図８】

英：A-Z、数：0-9	
4桁(英数)	1,679,616
5桁(英数)	60,466,176
6桁(英数)	2,176,782,336
7桁(英数)	78,364,164,096
8桁(英数)	2,821,109,907,456
4桁(数)	10,000
5桁(数)	100,000
6桁(数)	1000,000
7桁(数)	10,000,000
8桁(数)	100,000,000

【図９】


情報処理サーバ１
認証端末３
S104
リマインダー質疑応答記憶装置
S354
回答照合
リマインダー質疑応答登録
S301
質問と回答の選択肢の組合せを送信
S302
所定の数以上の質問と回答の組合せを送信
パスワード再発行
S351
パスワード再発行依頼
S352
質問と回答の選択肢の組合せを送信
S353
登録時に回答した質問と回答の組合せを送信
S355
パスワード再発行

【書類名】要約書
【要約】
【課題】認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理サーバ１を提供する。
【解決手段】情報処理サーバ１は、認証情報を記憶した認証識別子記憶装置１０３と、通信端末２の認証依頼を受信すると、生成した認証パラメータを含む認証画像を生成して通信端末２に送信し、認証パラメータを認証パラメータ記憶装置１０１に記憶する認証画像生成手段１１１と、通信端末２から取得した認証画像の情報と、認証端末３が備える認証情報を、認証端末３から取得する認証情報取得手段１１２と、認証パラメータ記憶装置１０１を参照して、認証情報取得手段１１２で取得した認証画像の情報が、認証画像生成手段１１１で生成された画像の情報であり、更に、認証端末３が備える認証情報が、認証識別子記憶装置１０３に記憶した認証情報と一致するか否かを判定し、その結果を通信端末２に送信する認証情報照合手段１１３とを備える。
【選択図】図１

特願２００３－３０７８７２

出 願 人 履 歴 情 報

識別番号 [５００２８５５６５]

１．変更年月日 ２０００年 ８月 ４日
[変更理由] 住所変更
住 所 東京都渋谷区広尾２丁目３番１４号
氏 名 北川 淑子